REMARKS

Claim 1 was pending in the application. Claim 1 was rejected. Claim 1 is amended. Claims 2-20 are added. Claims 1-20 are now pending in the application. Claim 1 is the independent claim. Reconsideration of the amended application is respectfully requested.

The examiner rejected claim 1 under 35 USC §102(e) as being anticipated by Fieres et al.

Amended claim 1 recites a process of checking the authorization and authenticity of an application for use by a user on a device within a domain. The process includes authenticating an application authentication file against a domain administrator's public membership key, checking the application authentication file for one or more application identification and authorization objects, and hashing an application executable. The application hash result is compared to an authentication hash contained in the application authentication file. Services to the application are denied if the application hash and the authentication hash do not match. The application identification and authorization objects are decoded if the application hash and the authentication hash match. The decoded application identification and authorization objects are compared to domain identification and authorization objects associated with the domain. Services are provided to the application if the result of the domain comparison is favorable, and services are denied to the application if the result of the domain comparison is not favorable.

Thus, claim one describes a process by which an application is checked for identity and authentication. The domain specifies which applications are valid for use

within the domain, and comparisons are made to determine that the application is allowed for use in the domain and that the application has not been changed since authorization. Claims 2-20 recite further checks, for example as to whether the user is identified and authenticated for use of the application, and authenticated for use of the application on the particular device.

In contrast, Fieres et al. discloses host system elements for an international cryptography framework. The application support elements include application authentication, by which a hash sum of the application code image, the application ID, and classes of service assigned to the application are authenticated by means of a digital signature. The class of service concept includes a trusted description of the application resource map and attributes that express the application's capabilities. The classes of service are mapped and analyzed when an application is called, so that suitable applications having the least capable classes of service are selected for a task. See column 8, line 47 through column 9, line 3; column 10, lines 45-59; and column 12, lines 11-20.

Thus, Fieres et al. do not disclose or suggest checking the identity and authentication of an application for valid use within a domain. Rather, Fieres et al. check attributes of an application to select a suitable and least-capable application for use in response to a call, and check the selected application for modification. Fieres et al. also do not disclose checking I&A attributes of a user and/or a device before allowing use of an application within the domain by the user on the user's device.

For at least the reasons noted above, Fieres et al. do not anticipate the invention as recited in claims 1-10. The rejection of claim 1, therefore, should be withdrawn.

Based on the foregoing, it is submitted that all objections and rejections have been overcome. It is therefore requested that the Amendment be entered, the claims allowed, and the case passed to issue.

Respectfully submitted,

June 10, 2005
Date

Thomas M. Champagne
Registration No. 36,478
IP STRATEGIES
12 ½ Wall Street
Suite I
Asheville, North Carolina 28801
828.253.8600
828.253.8620 fax

TMC:hlp